

## METHOD FOR REGULATING AND MANAGING USE OF VIRTUAL PRIVATE NETWORK AND ITS SYSTEM

Patent Number: JP2001251307  
Publication date: 2001-09-14  
Inventor(s): MIYOSHI JUN;; IMAIDA ISAMUNE;; KANEKO  
Applicant(s): NIPPON TELEGR & TELEPH CORP  
Requested Patent: ☐ JP2001251307  
Application: JP20000057568 20000302  
Priority Number(s):  
IPC Classification: H04L12/28; H04L12/56  
EC Classification:  
Equivalents:

---

### Abstract

---

**PROBLEM TO BE SOLVED:** To provide a method for regulating and managing use of a virtual private network and its system that can reduce a load of a broadband IP network and a VPN manager and operate an element control function on the basis of VPN utilization regulations.

**SOLUTION:** A policy storage section 13 stores a policy of a broadband IP network and a policy of a VPN, a policy verification function section 12 verifies a contradiction between the policy of the broadband IP network and a registration request of the policy of the VPN and a contradiction between regulations of use of the registered virtual private network and a service request from an end user, and the VPN policy is registered or set to a QoS controller 5 and a security controller 6 via a common platform section 14, a QoS policy control section 15 and a security policy control section 16 according to the result of verification.

---

Data supplied from the [esp@cenet](mailto:esp@cenet) database - 12



【特許請求の範囲】

【請求項1】 広域IP網上に構築され、運用される仮想プライベートネットワークにおける利用規定の管理方法であって、

複数の仮想プライベートネットワーク毎に定める利用規定の管理を行い、

仮想プライベートネットワーク間通信時のエンドユーザからのサービス要求を、要求元の仮想プライベートネットワークの利用規定と、通信相手先の仮想プライベートネットワークの利用規定との双方で検証することを特徴とする仮想プライベートネットワーク利用規定管理方法。

【請求項2】 仮想プライベートネットワークの利用規定を、広域IP網の管理者と、少なくとも1つの仮想プライベートネットワークの管理権限を持つ管理者とで階層的に管理することを特徴とする請求項1記載の仮想プライベートネットワーク利用規定管理方法。

【請求項3】 単一の仮想プライベートネットワークの管理権限を持つ管理者が複数の仮想プライベートネットワークを管理する場合、これらの仮想プライベートネットワーク間通信に関する仮想プライベートネットワークの利用規定を自動生成することを特徴とする請求項1記載の仮想プライベートネットワーク利用規定管理方法。

【請求項4】 エンドユーザからのサービス要求を、帯域保証制御や仮想プライベートネットワーク間接続に必要なセキュリティ制御等を行う各ネットワーク構成装置の制御装置の設定情報に変換して配信することを特徴とする請求項1記載の仮想プライベートネットワーク利用規定管理方法。

【請求項5】 広域IP網上に構築され、運用される仮想プライベートネットワークにおける利用規定の管理装置であって、

広域IP網の利用規定及び仮想プライベートネットワークの利用規定を格納する格納部と、

広域IP網の利用規定と仮想プライベートネットワークの利用規程との矛盾や登録済の仮想プライベートネットワークの利用規定とエンドユーザからのサービス要求との矛盾を検証する検証機能部と、

仮想プライベートネットワークの管理者からの利用規程の登録要求を受け付け、広域IP網の利用規定との検証結果に従って格納部に格納するとともに、エンドユーザからのサービス要求を受け付ける受付部と、

サービス要求の検証結果に従ってネットワーク構成装置の帯域保証制御装置及びセキュリティ制御装置に対する設定を行う制御部とを備えたことを特徴とする仮想プライベートネットワーク利用規定管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、広域IP(Internet Protocol)網上に構築され、運用

される仮想プライベートネットワークにおける利用規定の管理方法及びその装置に関するものである。

【0002】

【従来の技術】 ネットワーク(以下、NWと略記する。)における利用規程(以下、ポリシーと呼ぶ。)の管理技術については、情報処理学会シンポジウム論文集、vol. 98、No. 8、p41-48等において既知の技術として公開されており、また、IETF(The Internet Engineering Task Force)のPolicy Frameworkワーキンググループ(以下、policy WGと略記する。)等においてもポリシー管理技術に関する提案がなされている。

【0003】 しかし、これらの技術を用いた既存のNWポリシー管理装置はユーザNWに閉じた範囲を想定したものであり、ポリシー管理者及びエンドユーザという二層の管理構造しか持っておらず、また、仮想的な仮想プライベートネットワーク(以下、VPNと略記する。)を跨ったポリシーの管理は実現できていない。そのため、第1種及び第2種通信事業者等(以下、キャリアと呼ぶ。)が提供し、複数ユーザがリソースを共有する、IP over FR(Frame Relay)やIP over ATM等の広域IP網上にVPNが構築され、運用される場合、VPN間でポリシーの競合が発生する可能性があり、対応が困難であった。

【0004】 従来、広域IP網は全て広域IP網管理者が管理していたため、エンドユーザからのサービス要求はユーザ側のVPN管理者が仲介する形で、広域IP網管理者へ申し込みを行う必要があった。そのため、サービス要求発生から実際にサービス変更が行われるまでのタイムラグが大きく、仲介する要員の稼働が大きくなるという問題があった。

【0005】 従来の広域IP網上のVPNに対するサービス変更の流れの概略を図1に示す。

【0006】 運用中のNWについてのサービス要求はエンドユーザから発生する。具体的にはVPN間のフィルタリング解除要求や、帯域保証(またはサービス品質)(以下、QoSと略記する。)要求等である。VPN管理者は、これらのサービス要求を受け付け(S1)、自NWの利用規定に基づいてその要求に対する可否判断を行う(S2)。自NW内の構成装置(エレメント)に対してのみ変更の場合は自NW内で完結する(S3)が、広域IP網を跨る設定の場合はサービスを提供する広域IP網管理者へ依頼する必要がある(S4)。

【0007】 要求を受け取った広域IP網管理者(S5)は、広域IP網の利用規定に基づいてその要求に対する可否判断を行った(S6)後、必要ならサービス要求を実施し(S7)、完了報告を行う(S8)。完了報告を受けたVPN管理者はサービス要求が発生したエンドユーザに完了報告を行う(S9)。

【0008】

【発明が解決しようとする課題】このように、従来のNWポリシー管理装置では、VPN間相互接続の際、VPN間通信に双方のVPNポリシーを反映させることが困難であり、複数のVPN間でVPNポリシーの競合が発生する。このため、広域IP網管理者及びVPN管理者の調整移動が大きくなり、VPNの運用形態の変化に柔軟に対応することが困難であった。よって管理負担を軽減し、管理者のポリシーに基づいてNWを効率的に制御することが目的のNWポリシー管理装置を導入しても、効果が得られないという問題があった。

【0009】さらにサービス要求に対して、QoSやセキュリティ等の各エレメント制御機能を連携して制御する機能を有しておらず、それぞれのエレメントを制御するNWポリシー管理装置毎にポリシー設定及びサービス要求を行う必要があり、ポリシー設定に矛盾が発生する恐れのあることも問題であった。

【0010】本発明の目的は、広域IP網管理者及びVPN管理者の管理負担を軽減し、VPN管理者が規定したVPNポリシーに基づいてQoSやセキュリティ等のエレメント制御機能を運用できる、仮想プライベートネットワーク利用規定（VPNポリシー）管理方法及びその装置を提供することにある。

【0011】

【課題を解決するための手段】本発明では、前記課題を解決するため、広域IP網を管理するキャリア側の広域IP網管理者は広域IP網全体に関わるNW管理ポリシーを管理し、個々のVPN内のVPNポリシーについてはそれぞれのVPN管理者が管理する。このようにポリシーを階層的に管理することにより、VPN管理者は権限の範囲内でVPNの運用形態に応じた柔軟なVPNポリシーの設定、変更が可能となり、VPN管理者及び広域IP網管理者の管理負担を軽減できる。

【0012】また、VPNを跨るサービス要求が発生した場合は要求元のみならず、通信相手先のVPNポリシーとも照合を行うことにより、双方のVPNポリシーを反映したVPN間通信が可能となる。

【0013】また、単一のVPNの管理権限を持つ管理者が複数のVPNを管理する場合、該管理者が管理権限を持つVPN群をVPNグループとし、VPNグループ内のVPN間通信に関わるVPNポリシーの設定の矛盾を自動的に回避することにより、VPN間通信に関するポリシー設定作業を簡略化することができる。即ち、一方のVPNにおけるVPNポリシーをVPN管理者が設定し、その通信相手先のVPNが同一VPNグループ内であると判断された場合は、通信相手先のVPNにもVPN間通信に関するVPNポリシーを自動生成する。この際、各々のVPNが異なるアドレス体系を持つ場合も、アドレス変換情報を元にVPNポリシーの自動生成を行う。

【0014】さらに、エンドユーザから設定されるQoS及びVPNを跨った通信の要求を、これらのVPNポリシーで検証した後に、QoS制御やVPN間接続に必要なセキュリティ制御等を行う広域IP網における各ネットワークエレメントの制御装置の設定情報に変換して配信する。これにより、広域IP網上でQoSやセキュリティ等のネットワーク機能をポリシーに基づいて連携制御可能とする。

【0015】以上の過程をもって上記課題を解決する。

【0016】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

【0017】図2は本発明の実施の形態の一例を示すもので、複数のユーザ（もしくはユーザNW）1a, 1b, 1c及び2a, 2b, 2cがエッジルータ（ER）を介して広域IP網3に接続され、それぞれVPN#1及びVPN#2というWAN（Wide Area Network）を構成するネットワーク全体を示している。

【0018】本発明のVPNポリシー管理装置（以下、PMSと略記する。）10は、エッジルータを介して広域IP網3に接続されており、また、網管理用NW4というLAN（Local Area Network）にも接続されており、これを用いてNWを構成する各装置（エレメント）の制御装置との通信を行う（請求項4）。広域IP網管理者はPMS10のコンソール上において操作を行い、VPN管理者及びエンドユーザはVPN#1, VPN#2経由でPMS10に接続し、設定等の操作を行う。

【0019】NWポリシーを構成する情報はIETFのpolicy WGによって図3に示すように提案されており、本発明では各構成情報の管理者を図4に示すように階層化、即ちキャリア側の広域IP網管理者を広域IP網管理者、ユーザNW側管理者をVPN管理者として位置付け、それぞれのVPNポリシーについて広域IP網管理者は各VPN契約情報の管理を行い、VPN管理者は管理下にあるVPN内の帯域、セキュリティの運用ルールの管理を行うことにより、VPNポリシーの管理権限分散を行う。

【0020】これによって、従来のサービス要求の際に必要なとされた、広域IP網管理者とVPN管理者との間での申し込みや受付、エンドユーザとVPN管理者との間での申し込みや受付等、通常ルーチンで繰り返される手間が省かれることになる（請求項2）。

【0021】また、VPN間相互接続の際、VPNを跨るサービス要求が生じた場合、図5に示すように、ユーザが所属するVPNのポリシーだけでなく、通信相手先のVPNのポリシーを参照し(i)、双方で検証されることで、相互のVPNのポリシーに基づくセキュリティの高い通信が可能となる（請求項1）。

【0022】さらに、図5に示すように、企業内、学校内等で複数のVPNを部署毎、学部毎に契約している場合は複数のVPNをグループ化し、VPNグループとしてVPN管理者が複数VPNに跨るポリシーを扱うことを可能とする。これによりVPNグループ内でのVPN相互通信についてはVPNグループ内の1NW管理ポリシーとして登録し、ユーザ要求時にそれを参照する(i)ことで検証が行われ、VPNポリシーの登録と、PMS内での検証手順を簡略化できる(請求項2、3)。

【0023】図6はPMSの構成を示すもので、大きく分けて6つの機能ブロックからなっている。即ち、図中、11はユーザインタフェースを提供するポリシー受付部、12は要求された内容を検証するポリシー検証機能部、13はポリシー情報や操作記録を格納するデータベースのポリシー格納部、14は制御するネットワークエレメントとのやり取りのための共通プラットフォーム部、15はネットワークエレメントのQoSを制御するQoS制御装置5との通信を行うQoSポリシー制御部、16はネットワークエレメントのセキュリティを制御するセキュリティ制御装置6との通信を行うセキュリティポリシー制御部である。

【0024】本発明による広域IP網上のVPNに対するサービス変更に関わる各管理者及びユーザとPMSとのやり取りの概略を図7に示す。

【0025】また、図8は広域IP網ポリシー登録時のフローチャートを、図9はVPNポリシー登録時のフローチャートを、図10はユーザ要求発生時のフローチャートをそれぞれ示すもので、以下、本発明によるサービス変更について説明する。

【0026】ユーザがポリシーサービスの享受を希望した場合、キャリアである広域IP網管理者は広域IP網上においてVPNポリシーサービスのサービスユーザ情報の登録を行う。

【0027】まず、PMS10のポリシー受付部11を介してVPN及びVPNグループの情報を登録し(S11)、その管理者情報の登録を行う(S12)。その後、サービスの契約条件等に関わる広域IP網ポリシーを登録し(S13)、ポリシー格納部13に格納する(S14)。

【0028】上記にて登録されたVPN管理者はポリシー受付部11を介して自分が管理するユーザNWに対してのVPNポリシーのエントリ登録を行う(S21)。PMS10ではポリシー検証機能部12にて広域IP網ポリシーに照らし合わせ(S22)、広域IP網ポリシーに違反していないか判断する(S23)。

【0029】ここで、違反していた場合はエントリを中止し、ポリシー受付部11を介してVPN管理者にその旨を通知する(S30)。許可され、さらにエントリ登録されたVPNポリシーがVPNグループ内でのVPN間通信に関するものであると判断された場合(S24、

S25)は通信相手先VPNポリシーの自動生成を行う(S26)。この際、双方のVPNが異なるアドレス体系を用いている場合は、ポリシーに記述されたアドレスの変換も同時に行う。

【0030】さらに通信相手先VPNのVPNポリシー及び広域IP網ポリシーに照らし合わせ(S26)、許可されれば(S27)、ポリシー格納部13にVPNポリシーを格納し(S29)、拒否されればエントリを中止し、ポリシー受付部11を介してVPN管理者に結果を通知する(S30)。

【0031】なお、同一VPNグループ内でないVPN間通信と判断された場合(S24、S25)は、自VPNのVPNポリシーのみをポリシー格納部13に格納する(S29)。

【0032】エンドユーザがVPNポリシーサービスを楽しみたいと欲した場合、エンドユーザは利用要求をPMS10のポリシー受付部11に送る(S41)。PMS10は、まずポリシー検証機能部12にてエンドユーザが所属するVPNのVPNポリシーと利用要求の照合を行い(S42)、許可判断を行う(S43)。不許可の場合、その旨をポリシー受付部11を介してエンドユーザに通知して処理を終わる(S49)。許可された場合、その利用要求がVPNを跨るかどうかの判断を行う(S44)。

【0033】跨っていなければQoS・セキュリティ制御を行う(S48)。跨っていた場合、さらに要求がVPNグループを跨るかどうかの判断を行い(S45)、跨っていれば相手先VPNポリシーとの照合を行い(S46)、許可判断を行う(S47)。許可判断がされればQoS・セキュリティ制御を行い(S48)、結果通知を行う(S49)。

【0034】また、図11は前述したQoS・セキュリティ制御に関する詳細フローチャートを示すものである。

【0035】前述したステップS48で発出されたQoS・セキュリティ制御要求は共通プラットフォーム部14にてQoS及びセキュリティ成分に分解され(S51)、セキュリティ成分をセキュリティ制御装置6の設定情報に変換する(S52)。さらに、その設定情報が既にセキュリティ制御装置6に登録されている内容かどうかを判断し(S53)、未設定ならばセキュリティポリシー制御部16を介してセキュリティ制御装置6に設定する(S54)。

【0036】また、QoS成分をQoS制御装置5の設定情報に変換し(S55)、QoSポリシー制御部15を介してQoS制御装置5に設定する(S56)。設定結果はポリシー受付部11を介してユーザに通知される(S57)。

【0037】図12に登録されたVPNポリシーの閲覧画面の一例を、図13にエンドユーザからのサービス要

求の設定画面の一例を示す。

【0038】

【発明の効果】以上説明したように、本発明によれば、以下のような優れた効果を奏することができる。

(1) 複数ユーザでリソースを共有する広域IP網上で、各々のVPNの管理者のポリシーに基づいたセキュリティの高いVPN間通信を行うことが可能となる。

(2) VPNポリシーを階層的に管理することにより、VPN管理者は管理下にあるVPNのポリシーを柔軟に設定変更することが可能となり、VPN網管理者及び広域IP網管理者の稼働が軽減される。さらに、複数のVPNをグループ化し、仮想的な1つのVPNのように見せることでVPN間のアドレス空間の相違やフィルタリング設定等を意識することなく、一人のVPN管理者がVPN間通信のVPNポリシーを簡易に設定することが可能となる。

(3) VPNを跨るサービス要求に対し、QoS制御に連動したVPN間接続等のセキュリティ制御を自動的に行う等、異なるサービスを制御するエレメントの制御装置を連携制御することにより、設定稼働の軽減と矛盾のない設定が可能となる。

【図面の簡単な説明】

【図1】従来のサービス変更の流れの概略を示すフローチャート

【図2】本発明の実施の形態の一例を示すネットワーク構成図

【図3】IETF policy WGの提案におけるNWポリシーの構成情報を示す説明図

【図4】本発明による階層化されたVPNポリシー管理者と管理内容を示す説明図

【図5】VPNを跨ったサービス要求に対する検証のようすを示す説明図

【図6】本発明のVPNポリシー管理装置の機能ブロック図

【図7】本発明によるサービス変更に関わるやり取りの概略を示す説明図

【図8】広域IP網ポリシー登録時のフローチャート

【図9】VPNポリシー登録時のフローチャート

【図10】ユーザ要求発生時のフローチャート

【図11】QoS・セキュリティ制御に関する詳細フローチャート

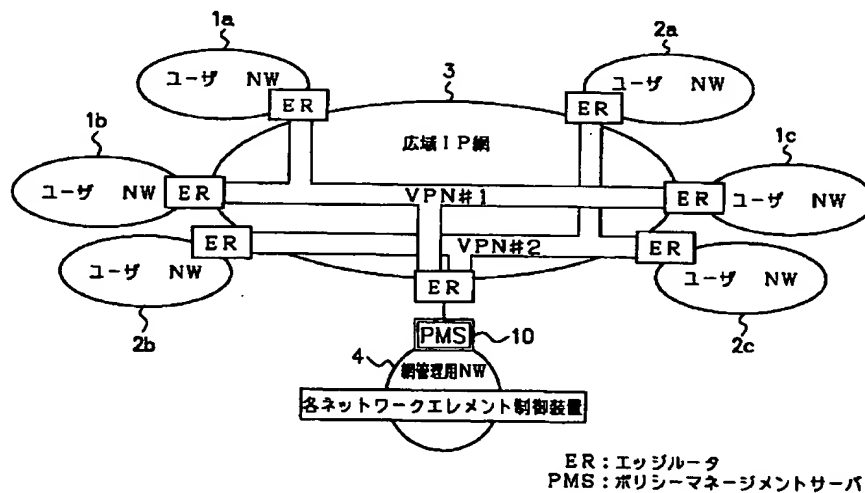
【図12】VPNポリシーの閲覧画面の一例を示す図

【図13】サービス要求の設定画面の一例を示す図

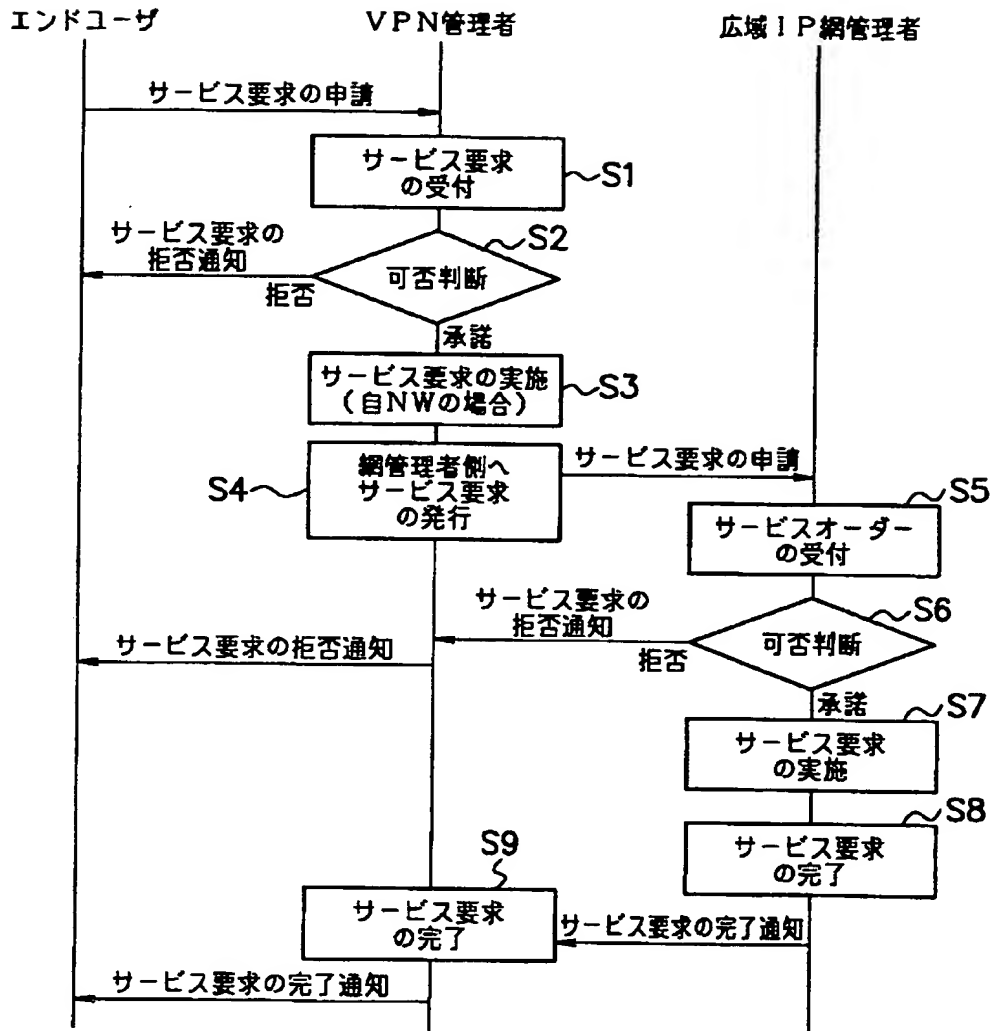
【符号の説明】

1a, 1b, 1c, 2a, 2b, 2c: ユーザ、3: 広域IP網、4: 網管理用NW、5: QoS制御装置、6: セキュリティ制御装置、10: VPNポリシー管理装置、11: ポリシー受付部、12: ポリシー検証機能部、13: ポリシー格納部、14: 共通プラットフォーム部、15: QoSポリシー制御部、16: セキュリティポリシー制御部。

【図2】



【図1】



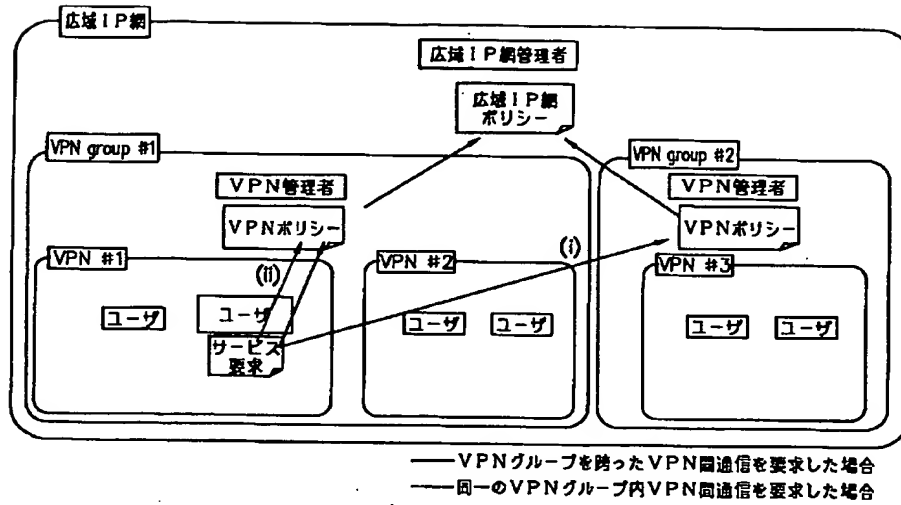
【図3】

構成情報名	構成情報内容
Policy Condition	送信側/受信側のIPアドレスやポート番号、プロトコルなど、制御の対象となるフローの情報を記述
Policy Action	割当てするQoS（優先度や帯域など）や通目の可否など、そのフローに対して行う制御内容を記述
Policy Time Period Condition	Policy Actionが適用される時間帯情報

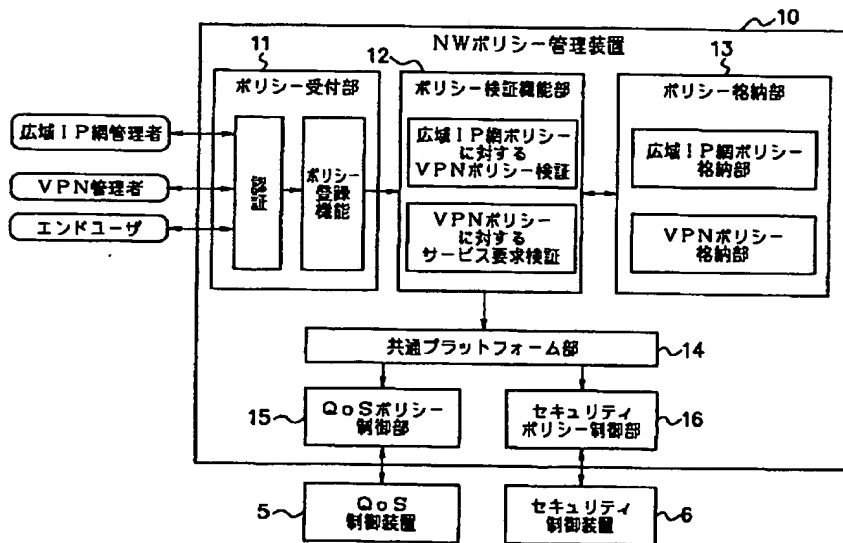
【図4】

管理者名	管理内容
広域IP網管理者	広域IP網ポリシー：各VPN契約情報 Policy Condition：VPNで定義されたアドレス空間 Policy Action：契約QoSクラス、契約帯域 Policy Time Period Condition：契約利用時間帯など
VPN管理者	VPNポリシー：管理下にある1または複数のVPN内の帯域、セキュリティなどの利用規定 Policy Condition：送信、受信ネットワークアドレス、アプリケーション Policy Action：利用可能QoSクラス、利用可能帯域 Policy Time Period Condition：利用可能時間帯
エンドユーザ	利用ポリシー：エンドユーザからのサービス利用要求 Policy Condition：送信、受信端末アドレス、アプリケーション Policy Action：要求QoSクラス、要求帯域 Policy Time Period Condition：利用希望時間帯

【図5】

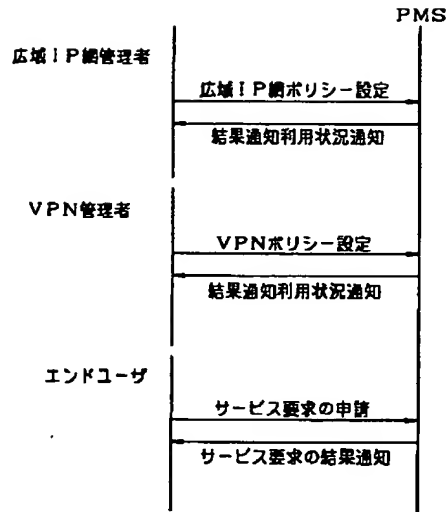


【図6】

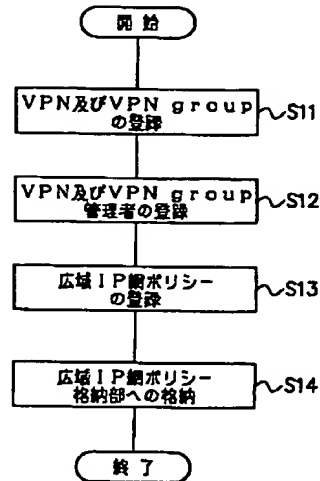




【図7】

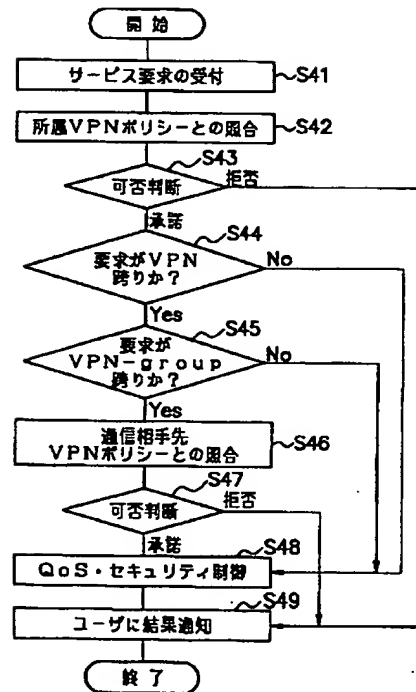
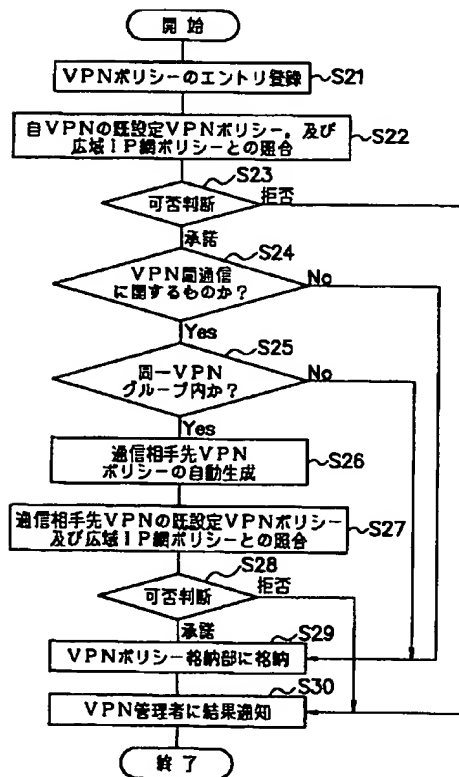


【図8】



【図10】

【図9】



TEL番号(リン-ネ)を入力  
7-0 (T) 88 (T) 96211 (A) 7-2 (T) 77 (R)  
☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐  
〒552-12

送信方向 ●片方向 ○双方向

最低先IPアドレス  プレフィックス長 ☐ 送信元ポート番号   
送信先IPアドレス  プレフィックス長 ☐ 宛先ポート番号

プロトコル ☒ TCP ☐ UDP

登録QoSクラス  17

要求速度  Kbps

最低許容速度  Kbps

サービス開始日時  年  月  日  時  分  
サービス終了日時  年  月  日  時  分

フロントページの続き

(72)発明者 金子 真也

大阪府大阪市中央区馬場町3番15号 西日

本電信電話株式会社内

F ターム(参考) 5K030 GA11 HA08 HC01 HD03 HD07

HD09 JA00 LB20 LC05 LD20

9A001 CC07 KK56 LL09